NADA Security Checklist to be completed and signed by Consultants

Version 1.0

Consultants tasked with installing the NADA software are required to complete and sign the following checklist and return it along with their mission reports to PARIS21\OECD.

- ☐ Directory browsing is off.
- ☐ The NADA database is set up with a NADA specific database user account and limited to only the necessary database permissions to run NADA. I.e. **Not ROOT (MySQL)** or the **SA account (MSSQL)**
- ☐ The database password is a minimum of 12 characters long. I.e. Contains capital letters, punctuation and numbers. Also, not a word found in a dictionary.
- ☐ You have asked the Client to set up a complex administrator password for NADA that **you** do not know. . I.e. Contains capital letters, punctuation and numbers. Also, not a word found in a dictionary.
- ☐ You have explained the importance of using complex passwords for administrator accounts and the importance of limiting the number of people who have an administrator account on the NADA.
- ☐ The NADA *datafiles* folder has been set up outside the web root.
- ☐ The NADA *cache* folder has been set up outside the web root.
- ☐ The NADA Logs folder has been set up outside the web root.
- ☐ The NADA *datafiles* folder has only READ and WRITE permissions set. Not Execute.
- ☐ The NADA *cache* folder has only READ and WRITE permissions set. Not Execute.
- ☐ The NADA *log* folder has only READ and WRITE permissions set. Not Execute.
- ☐ Any NADA administrator accounts set up for you have been deleted from the NADA.
- ☐ Any server administrator accounts set up for you have been deleted from the SERVER.

- [ ] If you were given Cpanel access by the client then you have asked them to change that password so you can no longer login.
- [ ] **All** applications such as phpMyAdmin installed by **you** to facilitate the installation have been uninstalled.
- [ ] Any files such as ones containing Phpinfo() or other scripts placed **by you** on the server to test the server environment have been removed. e.g. an info.php file.
- [ ] The Administrator URL has been customized and is not the default admin URL
- [ ] You have recommended that NADA be installed in a folder other than one called NADA. I.e. a custom URL is set.
- [ ] Instructions have been provided on how to backup the NADA files.
- [ ] Instructions have been provided on how to backup the NADA database.
- [ ] The NADA support contacts at the OECD and World Bank have been provided to the Client. Info@ihsn.org
- [ ] You have discussed the added security benefit of installing an SSL certificate for secure login and encouraged the Client to purchase one if possible.
- [ ] If an SSL certificate is available on the server then you have enabled HTTPS login in the NADA configuration.
- [ ] Discussed and made aware to the Client the general security good practice points below.

Name: Signature: Date:

Appendix: Resources

General good practice, resources and guides.

Web server and application security is important as breaches in security can lead to damage to the reputation of the organization.

- Don't install applications you don't need
- Remove all sample content (e.g. phpinfo) files and scripts used during development
- Disable services that are not needed for your a web server (e.g. ftp, LDAP, email server)
- Limit the number of users who have access to the server
- **Limit the roles of users on the server to the function they need to do (e.g. limit users who can start and stop services or alter directory or script permissions).**
- Limit folder permissions for script execution or web access to one directory only.
- Limit the uploading of files to directories that are not readable by the Web server. (in the case of NADA this would apply to the 'datafiles' folder).
- Enforce password expiration
- Enforce password complexity
- Remove users who no longer work with the organization
- Ensure programs\Operating System and applications are fully security patched at all times. E.g. PHP should, if possible, be the latest supported version available from php.net.
- Enable server and application logging
- Monitor that firewalls are working
- Keep Anti-virus software up-to-date
- Keep a fully backed up version of your server programs\ applications and websites in a secure place (not on the web server).
- Disable directory listing.

If you are hosting your site externally with an Internet Service Provider (ISP) then some of the application patching, logging and firewall security is taken care of by them, but others remain your responsibility.

Disable Directory listing on Apache

Disable directory browsing using .htaccess:

- **Open your .htacces file**
- Look for **Options Indexes**
- If **Options Indexes** exists modify it to **Options -Indexes** or else add **Options -Indexes** as a new line
- The directory browsing feature should now be disabled

Disable directory browsing using httpd.conf:

- Open your httpd.conf, normally it located at /usr/local/apache/conf or /etc/httpd.conf
- Go to your Virtual Host settings and look for "**Options Indexes**"
- Change the Indexes to **-Indexes** if Option Indexes exists or else add the **Options -Indexes** line
- Restart your apache web server.
- The directory browsing feature should now be disabled

Disable directory browsing in CPanel Share hosting environment:

- Login to your CPanel
- Click on **Index Manager**
- Click on the directory name for which you want to disable the directory browsing
- Select **No Index** and click Save

Disable Directory listing in Microsoft IIS 6, 7+

The methods used for this differ depending on the version of IIS you are using. Here are some resources you might find helpful.

http://technet.microsoft.com/en-us/library/cc731109(v=ws.10).aspx

http://www.iis.net/ConfigReference/system.webServer/directoryBrowse

http://technet.microsoft.com/en-us/library/cc732820.aspx

Creating user accounts and databases in MySQL

*Sample command sequence for setting up a **database** user for **the NADA** – the goal being to avoid using **Root** for your NADA configuration.*

From the command line type :

mysql -u root -p

- Enter your root password you setup when installing MySQL.
- Now create a database for the NADA – in this example we call the database nada

mysql> CREATE DATABASE nada;

- Now create a user who can access the new nada database and give the user only the rights necessary to run the NADA.

mysql> GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, INDEX, ALTER, CREATE TEMPORARY TABLES,LOCK TABLES ON nada.* TO 'nada'@'localhost' IDENTIFIED BY 'yourpassword';

- 'yourpassword' can be anything you choose. nada is the name of the database the user gets access to. localhost is the location which gets access to your database. Note: **remember this password** you will need it to configure your NADA installer! Then exit MySQL console by typing exit.

mysql> exit

Creating user accounts and databases in MSSQL

User and database security

- Never use the SA Account for running or setting up NADA
- More resources : http://msdn.microsoft.com/en-us/library/ms174173.aspx

Notes and warnings about phpMyAdmin

If **you** decide to install phpMyAdmin and to leave it installed on the server **(NOT RECOMMENDED)** then follow the following guide for securing it:

http://wiki.phpmyadmin.net/pma/Security

Again: the only applications **you** are authorized to install and leave on the server are the **database, php and NADA** software. If you need to, or are asked to, install phpMyAdmin then please mention the extra need to maintain password security, use SSL login and to never login as root from any place except the server itself. Tell your clients that if the database is accessed via phpMyadmin that their NADA and other sites could be compromised.